

epati

Active Directory - Kerberos SSO Configuration

Product: Antikor v2 - Next Generation Firewall
Configuration Examples

Active Directory - Kerberos SSO Configuration

Kerberos is an authentication protocol developed to prove the identity of resources that communicate on the network. SSO (Single Sign On) provides access by logging in with a single user ID.

Things to do on the Active Directory

1. A record must be entered on the DNS server in Domain Controller.

The screenshot shows the Windows DNS Manager interface. On the left, the tree view shows a domain structure with 'DNS' selected. Under 'DNS', there are several zones: '_msdc', '_sites', '_tcp', '_udp', 'DomainDnsZones', 'ForestDnsZones', '(same as parent folder)', '(same as parent folder)', '(same as parent folder)', 'antikor', 'epatitest', and 'testlocal'. The 'antikor' entry is highlighted. On the right, a table lists DNS records:

Name	Type	Data	Timestamp
Start of Authority (SOA)		[57] epatitest.sunucu.local...	static
Name Server (NS)		epatitest.sunucu.local.	static
Host (A)		192.168.100.10	6.05.2019 13:00:00
Host (A)		192.168.100.10	static
Host (A)		192.168.100.10	static
Host (A)		192.168.100.100	22.04.2019 16:00:00

A modal dialog box titled 'antikor Properties' is open, showing the 'Host (A)' tab. It contains the following fields:

- Host (uses parent domain if left blank): antikor
- Fully qualified domain name (FQDN): antikor.SUNUCU.LOCAL
- IP address: 192.168.100.10
- Update associated pointer (PTR) record

2. The a user named Antikor must be created in the Domain Controller.

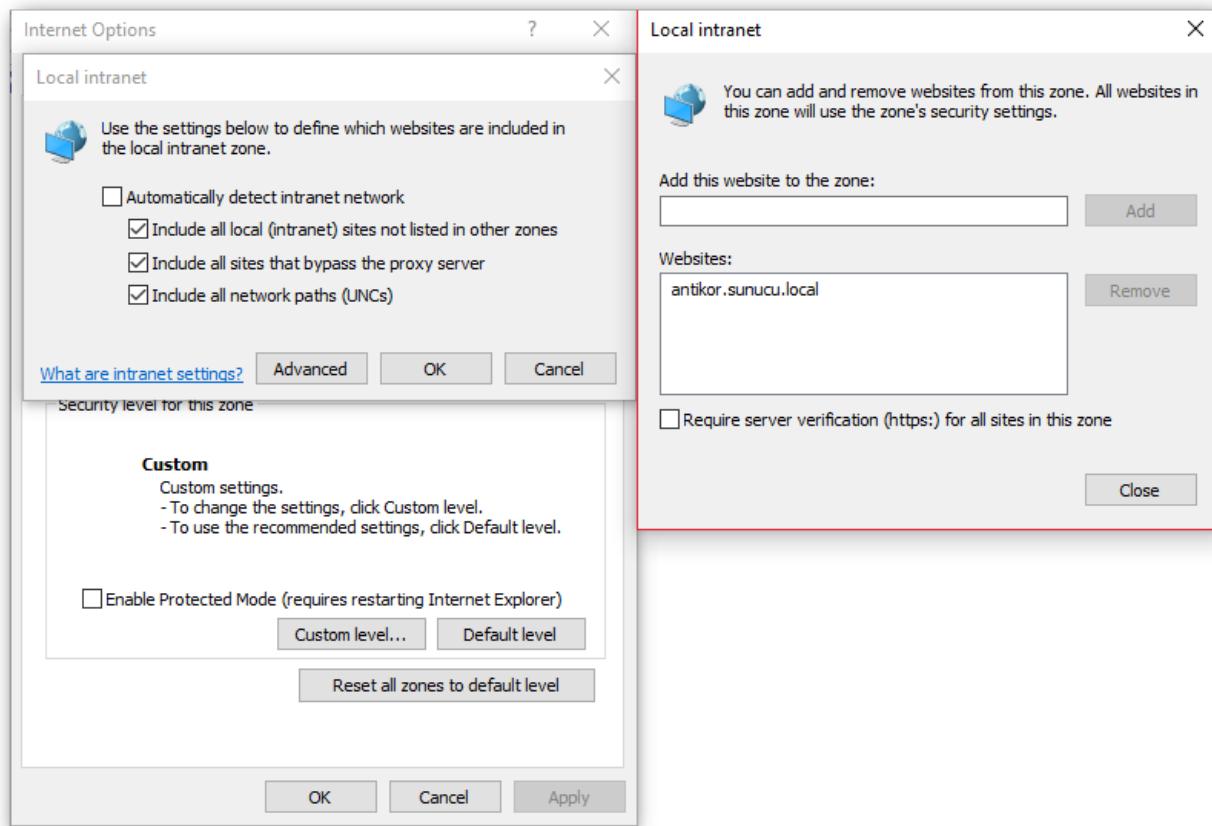
The screenshot shows the Active Directory Users and Computers snap-in. On the left, the navigation pane shows 'Active Directory Users and Computers' under 'Saved Queries'. Below it, the tree view shows the domain structure with 'SUNUCU.LOCAL' selected. Under 'Users', there is a list of existing users and groups. On the right, a 'New Object - User' dialog box is open. The 'Create in:' dropdown is set to 'SUNUCU LOCAL/Users'. The user information fields are filled as follows:

First name:	Antikor	Initials:	
Last name:			
Full name:	Antikor		
User logon name:	antikor	@SUNUCU.LOCAL	
User logon name (pre-Windows 2000):	SUNUCU\	antikor	

3. The CMD should be opened as an administrator and the keytab file should be created with the following command.

```
ktpass -princ HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL -mapuser antikor@SUNUCU.LOCAL -crypto all  
-ptype KRB5_NT_PRINCIPAL -pass SIFRE -out antikor.krb.keytab
```

4. antikor.SUNUCU.LOCAL should be written in the Internet Explorer > Security > Local Intranet > Sites > Advanced .



5. The Antikor SSL certificate must be distributed with Group Policy settings to all clients.

To add trusted sites using a GPO (Group Policy Objects), Launch Active Directory Users and Computers (ADUC), right click on the domain the clients are in, select Properties > Group Policy > New, type in a name for the GPO (like “IE Security Settings”) and then select Edit > User Configuration > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings. Select Import the current security zones and privacy settings > Modify Settings > Trusted Sites > Sites and add your Plexcel protected websites just as you would on a client. Then wait for the policy to propagate throughout the domain.

Things to do on the Antikor

1. The SUNUCU

.LOCAL record is must created on the Antikor Domain Definitions page.

Domain Definitions - New Record

Status	<input checked="" type="checkbox"/> Active
Domain Name	sunucu.local
DNS Server	IPv4 10.2.2.50

Cancel Save

2. Enter the record by selecting Provider Type SSO: Negotiate / Kerberos - Active Directory on the Identity Provider Definitions page.

Identity Provider Definitions - New Record

Status	<input checked="" type="checkbox"/> Active
Provider Type	SSO: Negotiate/Kerberos - Active Directory
Single Sign-on (SSO) may fail if a clock mismatch occurs with the Domain Controller / Kerberos Key Distribution Center. Please make sure that NTP synchronization is made in the Date Time Settings menu.	
Domain	SUNUCU.LOCAL
KDC / DC DNS Name	dc.SUNUCU.LOCAL
Antikor Assign DNS Name	antikor.SUNUCU.LOCAL

Cancel Save

3. The generated Keytab file will be uploaded via the Upload button. The Root Certificate button will appear if the "Single Sign-On SSO" option is enabled on the Verification Rules page.

6	<input checked="" type="checkbox"/> Active	SSO: Negotiate/Kerberos - Active Directory	SUNUCU.LOCAL	Edit	Delete	Upload	Root Certificate
---	--	--	--------------	-------------------	---------------------	---------------------	-------------------------------

When the Keytab file is loaded information like the following will appear;

Kerberos Keytab

Upload

Kerberos SSO Test

```
/antikor/etc/kerberos krb_VMoGgSjnOnmg.keytab:  
Vno Type Principal Aliases  
3 des-cbc-crc HTTP/antikor.sunucu.local@SUNUCU.LOCAL  
3 des-cbc-md5 HTTP/antikor.sunucu.local@SUNUCU.LOCAL  
3 arcfour-hmac-md5 HTTP/antikor.sunucu.local@SUNUCU.LOCAL  
3 aes256-cts-hmac-sha1-96 HTTP/antikor.sunucu.local@SUNUCU.LOCAL  
3 aes128-cts-hmac-sha1-96 HTTP/antikor.sunucu.local@SUNUCU.LOCAL
```

The Kerberos SSO Test button can be used for testing.

4. Once all the steps have been performed, the login process will be performed successfully.

Points to consider on the Antikor

1. NTP Server must be set.

Date/Time Settings

22.07.2019
14:32 24 +3

Get Automatically Active

Time Zones +3

NTP Servers

#	Status	Server Address	Transactions
1	Active	0.tr.pool.ntp.org	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Güncelle"/>
2	Active	1.tr.pool.ntp.org	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Güncelle"/>

XLS CSV PDF Filter Clear

2. The Single Sign-On SSO feature must be enabled on the Hotspot tab on the Verification Rules page..

Authentication Rules

Hotspot Proxy Registration Service L2TP / PPTP VPN SSL VPN RADIUS Client Change Form

Network All

0 Single Sign On SSO SUNUCU.LOCAL

1 Mernis

3. The date / time settings for the Domain Server, Client and Antikor must be the same.

4. IP addresses/IP block for SSO authentication should be added to on the Hotspot Clients page.

ePati Cyber Security Technologies Inc.
Mersin Universitesi Ciftlikkoy Kampusu
Teknopark Idari Binası Kat: 4 No: 411
Zip Code: 33343 Yenisehir / MERSIN / TURKIYE

www.epati.com.tr
 info@epati.com.tr
 +90 324 361 02 33
 +90 324 361 02 39

